UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,471	08/16/2001	Wei Xu	SNI-101B	1178

28970 7590 02/07/2005

SHAW PITTMAN
IP GROUP
1650 TYSONS BOULEVARD
SUITE 1300
MCLEAN, VA 22102

EXAMINER	
PATEL, ASHOKKUMAR B	

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 02/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/930,471	XU, WEI	
	Examiner	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-62* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-62* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/11/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Application Number 09/930, 471 was filed on 08/16/2001. Claims 1-62 are subject to examination.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-62 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-88 of copending Application No. 09/930, 272, claims 1-64 of copending Application No. 09/930, 141, claims 1-88 of copending Application No. 09/930, 164 and claims 1-66 of copending Application No. 09/ 930, 142. Although the conflicting claims are not identical, they are not patentably distinct from each other because the limitations of copending Application 09/ 930, 471 is overlapping the limitations of copending Applications as indicated above.

09/930, 471 Claims	09/930, 272 Claims	Differences and the reasons for obviousness.
1-13	1-16	Claims of the Application 09/930, 272 identify "third network application" receiving response from "second network application." While 09/930, 471 identify "second network application" receiving response from "first network application." It is well known in the art to have any number of applications serving the host. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add any number of applications since the network service can have more than two applications processing the data packets.
34-37	28-32	Same as above.
54-56	49-52	Same as above.
57-59	53-57	Same as above.
60-62	58-61	Same as above.
20-25	62	Same as above.
1-11	73	Same as above.

09/930, 471 Claims	09/930, 141 Claims	Differences and the reasons for obviousness.
1, 4-13	1, 3, 7,9	Claims of the Application 09/930, 141 identify "second network application" receiving the data packet by identifying the "second network application" based in part of the first network interface and second data packet address, while 09/930, 471 identifies "second network application" receiving response from "first network application." It is well known in art to identify the applications over the network by their addresses. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add any number of applications being identified by network interface addresses since the network service can have more than two applications processing the data packets.
1, 4-13	10-12	Same as above.
1, 4-13	50-52	Same as above.
1, 4-13	55-57	Same as above.
1, 4-13	60-62	Same as above.

09/930, 471 Claims	09/930, 164 Claims	Differences and the reasons for obviousness.
1	1, 7 and 8, 68-73, 79-84	Claims of the Application 09/930, 164 identify "second network application" though the response from "first network application." While 09/930, 471 identify "second network application" receiving response from "first network application." It is well known in the art to send data packet from one application to another. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to route the data packet to any number of applications since the network service can have more than two applications processing the data packets.
20	27-29	Same as above.

34-35	31-32	Claims of the Application 09/930, 164 identify "packet distribution entry" While 09/930, 471 identifies "packet sequencing entry." It is well known in the art to send packets from one application to another in an order. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to use and "term" the logic as being "packet distribution entry" rather than "packet sequencing entry." since it also allows the data packet being sequentially processed through different network applications.
54-57	53-56	Same as above for claims 1, 7 and 8.
1	53-62	Same as above for claims 1, 7 and 8.

09/930, 471 Claims	09/930, 142 Claims	Differences and the reasons for obviousness.
1-9	20-22, 52-54, 57-59, 62-64	Claims of the Application 09/930, 142 identify "service definition database" that includes plurality of network applications while 09/930, 471 provides the system that identifies the two network applications. It is well known in the art to have the routing oriented data that can be stored in the database. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to include this information in database for its instant availability for modifications and to route the data packet to any number of applications in a controlled manner since the network service can have more than two applications processing the data packets.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Attanasio et al. (US 5, 371, 852) (hereinafter Attanasio) in view of Shanklin et al. (hereinafter Shanklin) (US 6, 578, 147).

Referring to claim 1,

The reference Attanasio teaches "a method and apparatus for enabling a cluster of computers to appear as a single computer (a service address) to host computers outside the cluster. A host computer communicates only with a gateway to access destination nodes and processes within the cluster. The gateway has at least one message switch which processes incoming and outgoing port type messages crossing the cluster boundary. This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node. (Abstract and Fig. 4, col. 10, lines 63 through col.11, line 21) (A method of managing delivery of a network service, the method comprising: receiving a data packet, the data packet including a service address and a payload; identifying a plurality of network applications associated with the service address of the data packet, the plurality of network applications associated with the service address including a first network application and a second network application, the first network application being different than the second network application;)

Although the reference Attanasio teaches routing an incoming message to the proper computer node, port and process, the reference fails to teach sending at least the payload of the data packet to the first network application; receiving a first network application response packet from the first network application; and sending a second network application packet to the second network application, the second network application packet based at least in part on the first network application response packet.

The reference Shanklin teaches sending at least the payload of the data packet to the first network application (Fig. 5, element 51,"IDS Sensor"); receiving a first network application response packet from the first network application (Fig. 5, element P1, P4) ; and sending a second network application packet to the second network application, the second network application packet based at least in part on the first network application response packet. (Fig.5, element 54 i.e. to local network which is output of IDS Sensor 51, Note: The reference teaches

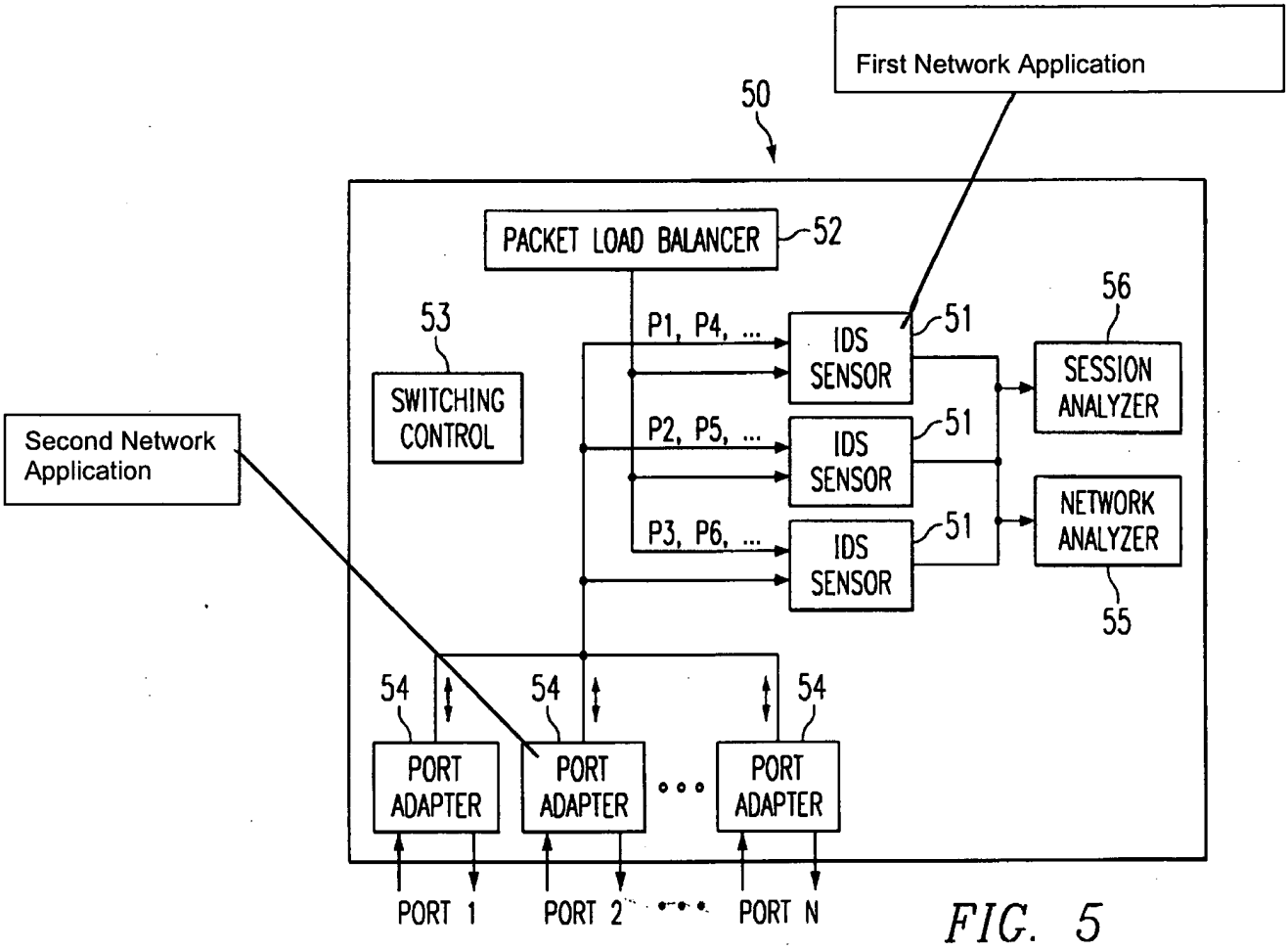

FIG. 5

Which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS

Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 2 and 3,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference fails to teach receiving a second network application response packet from the second network application; and sending a service response packet to a source address of the data packet, the service response packet based at least in part on the second network application response packet, and wherein sending a service response packet to a source address of the data packet includes generating the service response packet as a data product. The reference Shanklin teaches Fig. 5 configuration which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load

Balancer" and out to external network.) Thereby the reference teaches receiving a second network application response packet from the second network application; and sending a service response packet to a source address of the data packet, the service response packet based at least in part on the second network application response packet and wherein sending a service response packet to a source address of the data packet includes generating the service response packet as a data product.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claim 4,

The reference Attanasio teaches method of claim 1, wherein: the first network application has a first network application address; and sending at least the payload of the data packet to the first network application includes identifying the first network application address based at least in part on the service address. (Abstract," This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node.")

Referring to claims 5, 6 and 7,

Keeping in mind the teachings of the reference Attanasio as stated above in "Referring to claim 1", the reference Attanasio teaches "a method and apparatus for enabling a cluster of computers to appear as a single computer (a service address) to host computers outside the cluster. A host computer communicates only with a gateway to access destination nodes and processes within the cluster. The gateway has at least one message switch which processes incoming and outgoing port type messages crossing the cluster boundary. This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node. (Abstract and Fig. 4, col. 10, lines 63 through col.11, line 21) (wherein the first network application address is different from the first network application response source address, and wherein the first network application address is the same as the first network application response source address.). The reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, however, the reference explicitly fails to teach the first network application response packet includes a first network application response source address; the second network application has a second network application address; and sending a second network application packet to the second network application includes identifying the second network application address based at least in part on the first network application response source address.

The reference Shanklin teaches "For example, each sensor 21 or 31 might have a unique IP address so that routing is performed as with other IP-addressed

destinations.", col. 6, lines 34-37. The reference also teaches in Fig.5, elements 54 connecting to various nodes of Fig. 1. The reference Shanklin teaches Fig. 5 configuration which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.) Thereby the reference teaches the first network application response packet includes a first network application response source address; the second network application has a second network application address; and sending a second network application packet to the second network application includes identifying the second network application address based at least in part on the first network application response source address.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored by their source addresses as the flexibility provided by both references since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claim 8,

The reference Attanasio teaches wherein: the data packet includes a service port identifier; and sending at least the payload of the data packet to the first network application includes identifying the first network application address based at least in part on the service port identifier. (Abstract and col. 7, lines 34-35, Fig. 4)

Referring to claim 9,

The reference Attanasio teaches method of claim 4, wherein: the data packet is received on a first network interface; and sending at least the payload of the data packet to the first network application includes identifying the first network application address based at least in part on the data packet being received on the first network interface. (Abstract and col. 7, lines 34-35, Fig. 4, First network interface is the Cluster Gateway of Fig. 4)

Referring to claims 10 and 11,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, and receiving a data packet includes receiving a data packet via a first network interface; (Abstract and col. 7, lines 34-35, Fig. 4, First network interface is the Cluster Gateway of Fig. 4), however, the reference explicitly fails to teach receiving a data packet includes receiving a data packet via a first network interface; sending at least the payload of the data packet to the first network application includes sending at least the payload of the data packet to the first network application via a second network interface, the second network interface being different from the first network interface; and receiving a first network application response packet from the first network

application includes receiving the first network application response packet from a third network interface, the third network interface being different from the second network interface and the first network interface; and sending a second network application packet to the second network application includes sending the second network application packet to the second network application via a fourth network interface, the fourth network interface being different from the third network interface, the second network interface, and the first network interface, and receiving a second network application response packet from the second network application via the fourth network interface; sending a first network application return packet to the first network application via the third network interface, the first network application return packet based at least in part on the second network application response packet; receiving a first network application return response packet from the first network application via the second network interface; and sending a service response packet via the first network interface, the service response packet based at least in part on the first network application return response packet.

The reference Shanklin teaches "For example, each sensor 21 or 31 might have a unique IP address so that routing is performed as with other IP-addressed destinations.", col. 6, lines 34-37. The reference also teaches in Fig.5, elements 54 connecting to various nodes of Fig. 1. The reference Shanklin teaches Fig. 5 configuration which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network

10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.) Thereby the reference clearly teaches the claimed limitations as shown below.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored by their source addresses as the flexibility provided by both references since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

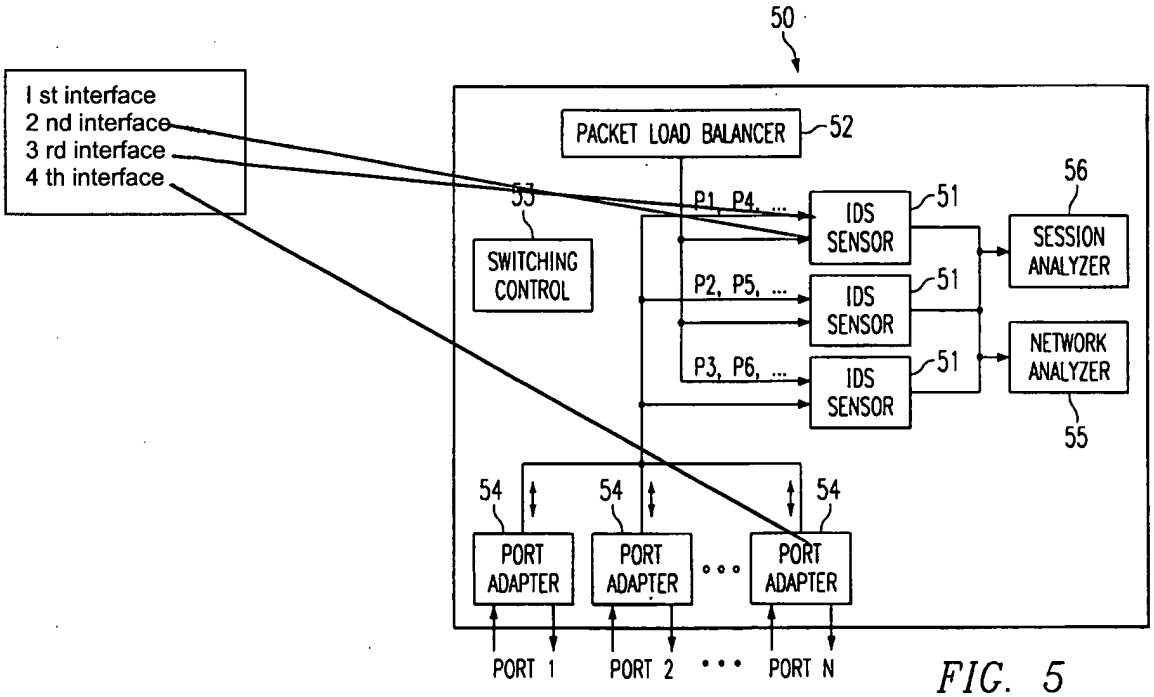

FIG. 5

Referring to claims 12 and 13,

The reference Attanasio teaches "a method and apparatus for enabling a cluster of computers to appear as a single computer (a service address) to host computers outside the cluster. A host computer communicates only with a gateway to access destination nodes and processes within the cluster. The gateway has at least one message switch which processes incoming and outgoing port type messages crossing the cluster boundary. This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node. (Abstract and Fig. 4, col. 10, lines 63 through col.11, line 21).Thereby the reference teaches the data packet includes a service port identifier; identifying the first network application address is based at least in part on the service port identifier and receiving a data packet includes receiving a data packet via a first network interface.

Although the reference Attanasio teaches routing an incoming message to the proper computer node, port and process, the reference fails to explicitly teach the first network application having a first network application address; and sending at least the payload of the data packet to the first network application includes identifying the first network application address based at least in part on the service address of the data

packet and the first network interface, and sending at least the payload of the data packet to the first network application via a second network interface, the second network interface being different than the first network interface.

The reference Shanklin teaches sending at least the payload of the data packet to the first network application (Fig. 5, element 51,"IDS Sensor"); receiving a first network application response packet from the first network application (Fig. 5, element P1, P4) ; and sending a second network application packet to the second network application, the second network application packet based at least in part on the first network application response packet. (Fig.5, element 54 i.e. to local network which is output of IDS Sensor 51, Note: The reference teaches in Fig.5, which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.) Thereby, as explained above, the reference teaches the first network application having a first network application address; and sending at least the payload of the data packet to the first network application includes identifying the first network application address based at least in part on the service address of the data packet and the first network interface, and sending at least the payload of the data packet to the

first network application via a second network interface, the second network interface being different than the first network interface, and wherein the data packet includes a service port identifier; identifying the first network application address is based at least in part on the service port identifier.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 14 and 15,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, the reference fails to teach sending at least the payload of the data packet to the first network application is based at least in part on a stateless identification of the first network application; and sending a second network application packet to the second network application is based at least in part on a stateless identification of the second network application, and wherein: sending at least the payload of the data packet to the first network application is based at least in part on a stateful identification of the first network application; and sending a second network application packet to the second network application is based at least in part on a stateful identification of the second network application. The reference Shanklin teaches these limitations col.6, lines 25-56.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 16 ,17 and 18,

Keeping in mind the teachings of the reference Attanasio as stated above, although the reference teaches "This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node"(Abstract), the reference fails to explicitly teach wherein the first network application is a first version of a network application and the second network application is a second version of the network application, and, wherein the first version of the network application is from a first vendor, the second version of the network application is from a second vendor, and the first vendor is different from the second vendor and wherein the network application is selected from the group consisting of an intrusion detection application, a virus detection application, a virtual private network application, a firewall application, a web switch, a network security application, a load balancing application, a proxy application, and a database application. The reference Shanklin teaches the claimed elements by teaching the first application being IDS sensor, element 11 and second application being server 10 in Fig. 1 which is also presented in different configuration in Fig. 5.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound from different applications, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claim 19,

Keeping in mind the teachings of the reference Attanasio as stated above, although the reference teaches "This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node" (Abstract), the reference fails to explicitly teach the first network application is selected from the group consisting of an intrusion detection application, a virus detection application, a virtual private network application, a firewall application, a web switch, a network security application, a load balancing application, a proxy application, and a database application; and the second network is a different network application selected from the group consisting of an intrusion detection application, a virus detection application, a virtual private network application, a firewall application, a web switch, a network security application, a load balancing application, a proxy application, and a database application. The reference Shanklin teaches the first application being IDS sensor, element 11 and second application being server 10 (database application or a virtual

private network application or network security application) in Fig. 1 which is also presented in different configuration in Fig. 5.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound from different applications, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 20, 21, 22, 23, 24 , 25, 28 and 29,

Keeping in mind the teachings of the reference Attanasio as stated above, although the reference teaches "This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node (Abstract). The reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35. Also refer to Abstract and Fig. 4, col. 10, lines 63 through col.11, line 21) Thereby the reference teaches receiving a first data unit at a first network interface, the first data unit including a service address; identifying a plurality of application systems based at least in part on the service address, the plurality of application systems including a first application system and a second application system. The reference explicitly fails to explicitly teach the remaining claimed limitations.

The reference Shanklin teaches, as shown below , sending at least the payload of the data packet to the first network application (Fig. 5, element 51,"IDS Sensor"); receiving

a first network application response packet from the first network application (Fig. 5, element P1, P4) ; and sending a second network application packet to the second network application, the second network application packet based at least in part on the first network application response packet. (Fig.5, element 54 i.e. to local network which is output of IDS Sensor 51, Note: The reference teaches Fig. 5, which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

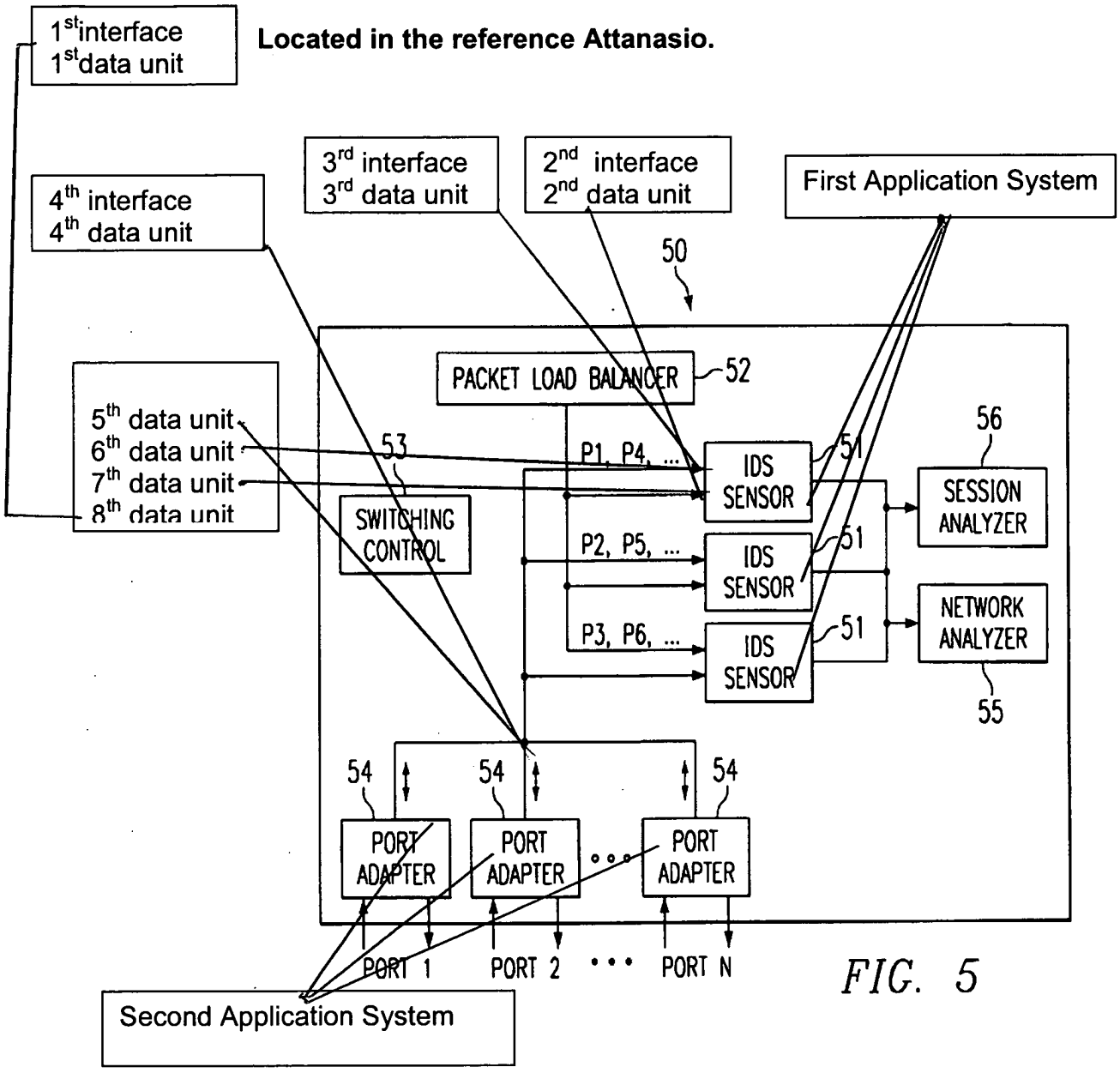

FIG. 5

Referring to claims 26 and 27,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, the reference fails to teach wherein identifying the first application system is based at least in part on a stateless identification of the first application system. (col. 7, lines 30-37), and wherein identifying the first application system is based at least in part on a stateful identification of the first application system. The reference Shanklin teaches these limitations col.6, lines 25-56.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claim 30, 31, 32 and 33

The reference Attanasio teaches "a method and apparatus for enabling a cluster of computers to appear as a single computer (a service address) to host computers outside the cluster. A host computer communicates only with a gateway to access destination nodes and processes within the cluster. The gateway has at least one message switch which processes incoming and outgoing port type messages crossing the cluster boundary. This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node. (Abstract and Fig. 4,

col. 10, lines 63 through col.11, line 21) (a method to manage delivery of a network service, the method comprising: receiving a data packet having a service address and a service port identifier; identifying a plurality of network applications based at least in part on the service address, the plurality of network applications including at least a first network application and a second network application; receiving a data packet having a service address and a service port identifier includes receiving the data packet via a first network interface;) However, the reference fails to explicitly teach sequentially processing the data packet through at least the first network application and the second network application based at least in part on the service address and the service port identifier; and sending a data packet service response based at least in part on the data packet sequential processing and wherein sequentially processing the data packet through at least the first network application and the second network application consists essentially of statelessly sequentially processing the data packet through at least the first network application and the second network application and remaining claimed elements pf claims 31, 32 and 33.

The reference Shanklin teaches sending at least the payload of the data packet to the first network application (Fig. 5, element 51,"IDS Sensor"); receiving a first network application response packet from the first network application (Fig. 5, element P1, P4) ; and sending a second network application packet to the second network application, the second network application packet based at least in part on the first network application response packet. (Fig.5, element 54 i.e. to local network which is output of IDS Sensor 51, Note: The reference teaches

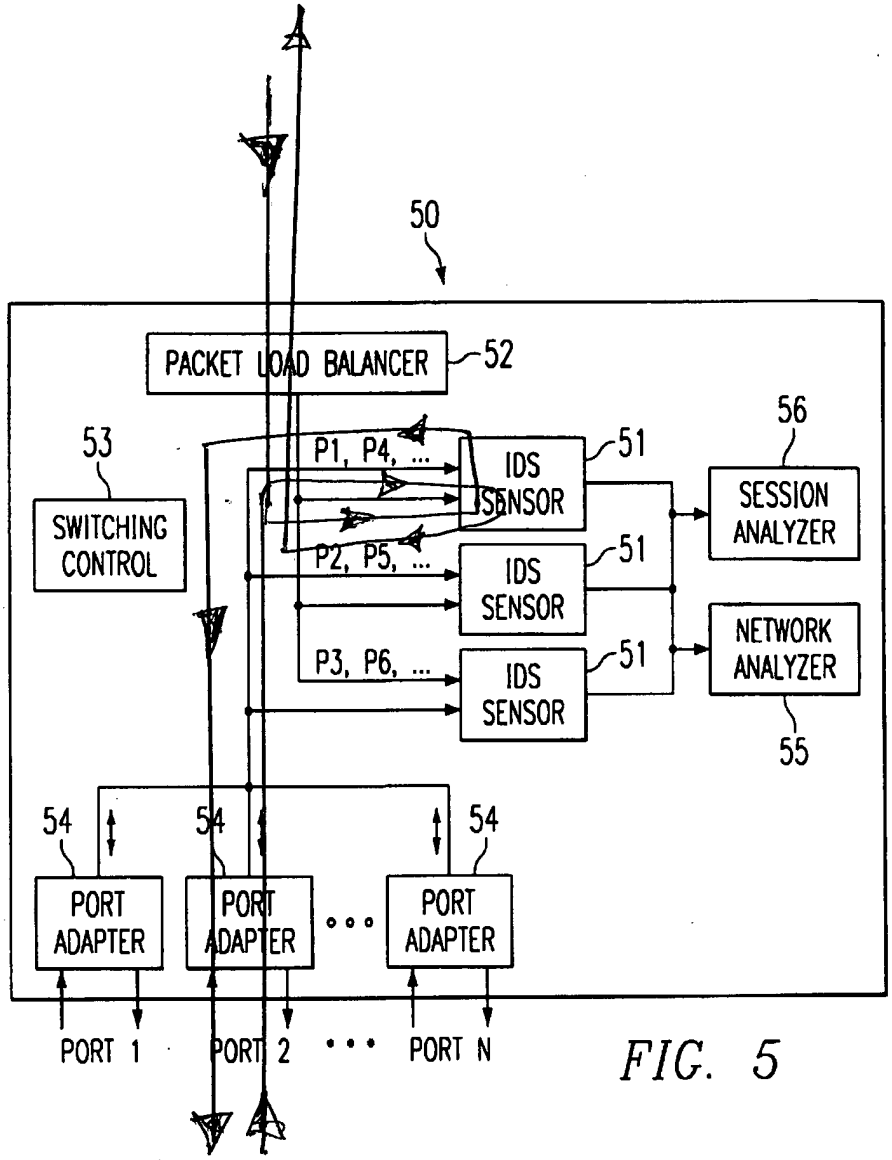

FIG. 5

Which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the

path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.)(sequentially processing the data packet through at least the first network application and the second network application based at least in part on the service address and the service port identifier; and sending a data packet service response based at least in part on the data packet sequential processing.) The reference Shanklin teaches "wherein sequentially processing the data packet through at least the first network application and the second network application consists essentially of statelessly sequentially processing the data packet through at least the first network application and the second network application" in col.6, lines 25-56.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 34 and 42,

keeping in mind the teachings of the reference Attanasio as stated above, The reference Attanasio also teaches a system to manage delivery of a network service (Fig.4) , the system comprising: a first network interface to receive a data packet, the data packet including a service address; packet sequencing logic to store packet sequential processing information, the packet sequential processing information

including a service address field to store a service address, the packet sequential processing information including a plurality of packet sequencing entries, one or more of the packet sequencing entries of the plurality of packet sequencing entries including a source address field to store a source address, and a destination address to store a destination address ; (Fig. 4, element 400) and "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35. The reference fails to explicitly teach a second network interface to transmit at least the payload of the data packet to a first network application system of a plurality of network application systems associated with the service address, the second network interface being different from the first network interface; a third network interface to receive a first network application response packet, the third network interface being different from the second network interface and the first network interface; and a fourth network interface to send a second network application packet to a second network application system of the plurality of network application systems associated with the service address, the second network application packet based at least in part on the first network application response packet, the second network application system being different from the first network application system, the fourth network interface being different from the third network interface, the second network interface, and the first network interface.

The reference Shanklin teaches sending at least the payload of the data packet to the first network application (Fig. 5, element 51,"IDS Sensor"); receiving a first network application response packet from the first network application (Fig. 5, element P1, P4) ; and sending a second network application packet to the second network application, the

second network application packet based at least in part on the first network application response packet. (Fig.5, element 54 i.e. to local network which is output of IDS Sensor 51, Note: The reference teaches

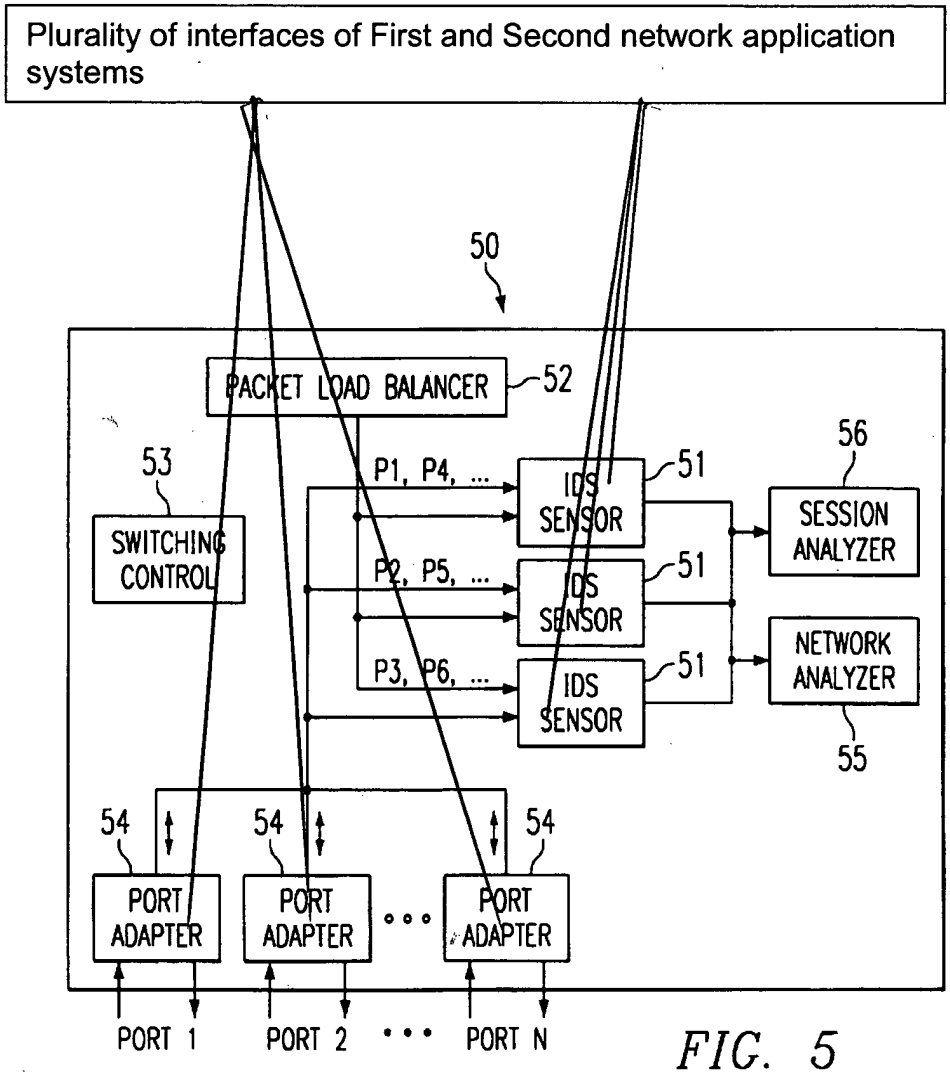

FIG. 5

Which is internal to the switch of Fig. 1, element 12, which is internetworking device (col.3, lines 30-39, note: "Router 12 inspects packets incoming from the external network to determine which should be forwarded into the local network 10. Similarly, packets originating in the local network are inspected to determine whether they are to be forwarded to the external network." And as clearly indicated by the Figure 5, the path of the packet is shown by the arrows traveling from "Packet Load Balancer" to "IDS Sensor" to "Port Adapter" and back from "Port Adapter" to "IDS Sensor" to "Packet Load Balancer" and out to external network.)(a second network interface to transmit at least the payload of the data packet to a first network application system of a plurality of network application systems associated with the service address, the second network interface being different from the first network interface; a third network interface to receive a first network application response packet, the third network interface being different from the second network interface and the first network interface; and a fourth network interface to send a second network application packet to a second network application system of the plurality of network application systems associated with the service address, the second network application packet based at least in part on the first network application response packet, the second network application system being different from the first network application system, the fourth network interface being different from the third network interface, the second network interface, and the first network interface.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway

such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claim 31,

Referring to claim 35,

The reference Attanasio teaches the system of claim 34, wherein one or more of the packet sequencing entries of the plurality of packet sequencing entries include: a received interface field to store a received interface identifier; and a send interface field to store a send interface identifier. (Fig.4, element 400, col. 11, lines 21-42)

Referring to claim 36,

The reference Attanasio teaches the system of claim 34, wherein: the data packet includes a first service port identifier, and one or more packet sequencing entries of the plurality of packet sequencing entries include a service port field to store a service port identifier. (Fig.4, element 400, col. 11, lines 21-42)

Referring to claim 37,

The reference Attanasio teaches the system of claim 34, wherein: the data packet includes a first service port identifier; and one or more packet sequencing entries of the plurality of packet sequencing entries include a received interface field to store a received interface identifier, a service port field to store a service port identifier, a send interface field to store a send interface identifier, and a send address field to store a send address. (Fig.4, element 400, col. 11, lines 21-42)

Referring to claim 38,

The reference Attanasio teaches the system of claim 37, wherein the send address is a network address of a network application system of the plurality of network application systems. (Abstract and Fig.4, element 400, col. 11, lines 21-42)

Referring to claim 39,

The reference Attanasio teaches the system of claim 37, wherein the send address is a media access controller address of a network application system of the plurality of network application systems. (Abstract, "This processing comprises examining certain information on the message headers and then changing some of this header information either to route an incoming message to the proper computer node, port and process or to make an outgoing message appear as if originated at the gateway node.")

Referring to claim 40,

The reference Attanasio teaches the system of claim 37, wherein each packet sequencing entry of the plurality of packet sequencing entries includes a destination system type field to store a destination system type identifier.(Abstract and Fig.4, element 400, col. 11, lines 21-42).

Referring to claim 41,

The reference Attanasio teaches the system of claim 34, wherein the first network application system is a first implementation of one network application system and the second network application system is a second implementation of the one network application system. (Fig. 2, element 200)

Referring to claims 43 and 44,

Claims 43 and 44 are claims to a system that carry out the methods of claims 18 and 19. Therefore claims 43 and 44 are rejected for the reasons set forth for claims 16, 17, 18 and 19.

Referring to claims 45, 46 and 47,

The reference Attanasio teaches the system of claim 34, wherein the data packet uses one or more protocols from one of a TCP/IP network protocol suite and a UDP/IP network protocol suite, and wherein the one or more protocols include an IPv4 network protocol, and wherein the one or more protocols include an IPv6 network protocol. (col. 7, lines 14-63).

Referring to claims 48, 49 and 50,

The reference Attanasio teaches the system of claim 34, wherein the data packet uses one or more of a layer 2 protocol, a layer 3 protocol, and a layer 4 protocol, and wherein the layer 2 protocol is selected from the group consisting of ATM and frame relay, and wherein the layer 3 protocol is MPLS. (col. 8, lines 3 through col. 10, line 62).

Referring to claims 51, 52 and 53,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, the reference fails to teach the system of claim 34, wherein the packet sequential processing information lacks information that supports stateful processing, and wherein the packet sequential processing information includes information that supports stateful processing, and , wherein the packet sequential

processing information consists essentially of information that supports stateless processing. The reference Shanklin teaches these limitations col.6, lines 25-56.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 54 and 56,

Claims 54 and 56 are claims to the system that carries out the methods of claims 30 and 32. Therefore claims 54 and 56 are rejected for the reasons set forth for claims 30 and 32.

Referring to claim 55,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, the reference fails to teach the system of claim 54, wherein the means for sequentially processing the data packet through at least the first network application and the second network application includes means for statelessly sequentially processing the data packet through at least the first network application and the second network application. The reference Shanklin teaches these limitations col.6, lines 25-56.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway

such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 57 and 59,

Claims 57 and 59 are claims to the steps that carries out the methods of claims 30 and 32. Therefore claims 57 and 59 are rejected for the reasons set forth for claims 30 and 32.

Referring to claim 58,

Keeping in mind the teachings of the reference Attanasio as stated above, the reference also teaches "Internal IP addresses are assigned to the nodes of the cluster.", col. 7, lines 34-35, the reference fails to teach the method of claim 57, wherein the step for sequentially processing the data packet through at least the first network application and the second network application includes a step for statelessly sequentially processing the data packet through at least the first network application and the second network application. The reference Shanklin teaches these limitations col.6, lines 25-56.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement Shanklin's switch into Attanasio's gateway such that all traffic, outbound as well as inbound, is monitored since it provides a processor based intrusion detection which keeps up with the high traffic throughput of today's network as taught by Shanklin.

Referring to claims 60 and 62,

Claims 60 and 62 are claims to computer-readable medium storing a plurality of instructions to be executed by a processor to manage delivery of a network service in accordance with the method of claims 30 and 32. Therefore claims 60 and 62 are rejected for the reasons set forth for claims 30 and 32.

Referring to claim 61,

Claim 61 is a claim to the computer-readable medium storing a plurality of instructions to be executed by a processor to manage delivery of a network service in accordance with the method of claims 31. Therefore claim 61 is rejected for the reasons set forth for claims 30, 31, 32 and 34

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on (571) 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100